A POSITIVE-DEFINITE TERNARY QUADRATIC FORM DOES NOT REPRESENT ALL POSITIVE INTEGERS

Greg Doyle
School of Mathematics and Statistics, Carleton University, Ottawa, Canada
gregorydoyle@hotmail.com

Kenneth S. Williams
School of Mathematics and Statistics, Carleton University, Ottawa, Canada
kennethwilliams@cunet.carleton.ca

Received: 1/1/17, Accepted: 9/22/17, Published: 10/6/17

Abstract

Let Q be a positive-definite integral ternary quadratic form. We give a new elementary proof that Q cannot represent all positive integers by explicitly exhibiting an infinity of positive integers not represented by Q. We do this using only simple congruence properties. The principal idea is showing that the congruence

$$ax^2 + by^2 + cz^2 \equiv -4abc \pmod{32(abc)^2}$$

has no solutions $(x, y, z) \in \mathbb{Z}^3$ for any positive integers a, b and c.

1. Introduction

Let $\mathbb{N}, \mathbb{N}_0$ and $\mathbb{Z}$ denote the sets of positive integers, non-negative integers and integers, respectively. Let $Q(x, y, z)$ be an integral ternary quadratic form, that is

$$Q = Q(x, y, z) := ax^2 + by^2 + cz^2 + dxy + exz + fyz,$$

where $a, b, c, d, e, f \in \mathbb{Z}$. The form Q is said to be diagonal if $d = e = f = 0$ and classically integral if d, e and f are even. We assume that Q is positive-definite, that is $Q(x, y, z) > 0$ for all integers x, y, z with $(x, y, z) \neq (0, 0, 0)$. A positive integer n is said to be represented by Q if $Q(x, y, z) = n$ for some $x, y, z \in \mathbb{Z}$. Any form Q which represents all positive integers is said to be universal, and if Q fails to represent at least one positive integer it is called non-universal. The following result is classical.

Theorem. *A positive-definite integral ternary quadratic form is non-universal.*

Unfortunately we do not know who originally proved this result. Dickson [5, Vol. III, Chap IX] describes the contributions of the first mathematicians to study ternary quadratic forms (Gauss, Seeber, Dirichlet, Hermite, Eisenstein, Smith, Meyer, Mordell and Humbert) but this result is not mentioned. The first explicit statement of this result that the authors can find is by Albert in 1933 for classically integral forms, see [1, Theorem 13, p. 291]. Albert states that this result is well-known but does not provide a reference. He proves it in an elementary manner as a consequence of his study of the integers represented by the set of all positive-definite classically integral ternary quadratic forms of the same determinant. The only other explicit statement of this result that the authors found is at the end of Conway's book [3, p. 142] where he gives a modern proof using the concepts of isotropic forms and the p-adic equivalence of forms. However, there are stronger results in the literature from which the result can be deduced. We give just two examples.

Kaplansky [7] in 1995 determined all the possible classes of positive-definite integral ternary quadratic forms which represent all odd positive integers. There are 23 of them. It is easy to check that each of these 23 forms fails to represent at least one even positive integer. Thus it follows that no positive-definite integral ternary quadratic form is universal. Kaplansky's paper is written in a somewhat informal style, and not all the details of the proofs and calculations are given, for example "The investigation involved a fair amount of hand computation which, I feel, is unsuitable for public scrutiny" [7, p. 210].

Conway in his book [3, pp. 81-82] proves that if G is a positive-definite integral ternary quadratic form that represents all the integers $1, 2, \ldots, 30$ then G is equivalent to the form $x^2 + 2y^2 + 4z^2 + yz$. But $x^2 + 2y^2 + 4z^2 + yz$ does not represent 31 so again the non-universality of G follows as a corollary. Conway uses his own "topographs" as well as some inequalities of Minkowski to prove his result in a somewhat brief manner.

In view of this background it seemed desirable to us to give a stand-alone, direct elementary proof of this result using only elementary methods in number theory such as those found in an introductory number theory course. The objective of this paper is to give such a proof. We begin by looking at diagonal positive-definite integral ternary quadratic forms $ax^2 + by^2 + cz^2$. We show, using no more than congruences and the law of quadratic reciprocity, that no positive integer congruent to $-4abc$ modulo $32(abc)^2$ can be represented by $ax^2 + by^2 + cz^2$ (see Theorem 1 and Corollary 1). (Dickson in his book [4, p. 104] shows that the diagonal ternary quadratic form $ax^2 + by^2 + cz^2$ $(a, b, c \in \mathbb{N})$ is non-universal but does not exhibit an infinity of positive integers not represented by $ax^2 + by^2 + cz^2$.) Then we deduce the analogous result for non-diagonal ternary forms Q from the diagonal case. We explicitly exhibit a full congruence class of positive integers which is not represented by the perfectly arbitrary positive-definite integral ternary quadratic

form Q in terms of its coefficients (see Theorem 3). This shows that Q cannot represent every positive integer and in fact it fails to represent an infinity of them.

The central idea of our proof of the non-universality of a ternary form is the following theorem, whose proof is completed in sections $2-4$.

Theorem 1. *Let $a, b, c \in \mathbb{N}$. Then the congruence*

$$ax^2 + by^2 + cz^2 \equiv -4abc \pmod{32(abc)^2}$$

is insolvable in integers x, y and z.

Immediately from Theorem 1 we obtain the following result, which establishes the non-universality of the diagonal ternary form $ax^2 + by^2 + cz^2$ $(a, b, c \in \mathbb{N})$.

Corollary 1. *Let $a, b, c \in \mathbb{N}$. Then the ternary form $ax^2 + by^2 + cz^2$ does not represent any of the positive integers*

$$4abc(8abck - 1), \quad k \in \mathbb{N}.$$

From Theorem 1 we deduce the following theorem.

Theorem 2. *Let $a, b, c \in \mathbb{N}$. Define positive integers r and s uniquely by*

$$abc = r^2 s, \quad s \text{ squarefree.}$$

Then the congruence

$$ax^2 + by^2 + cz^2 \equiv -s \pmod{8abcs}$$

is insolvable in integers x, y and z.

Proof. Suppose that X, Y, Z are integers such that

$$aX^2 + bY^2 + cZ^2 \equiv -s \pmod{8abcs}.$$

Define integers x, y, z by

$$x = 2rX, \quad y = 2rY, \quad z = 2rZ.$$

Then

$$ax^2 + by^2 + cz^2 = 4r^2(aX^2 + bY^2 + cZ^2) \equiv -4r^2 s \pmod{4r^2 \cdot 8abcs},$$

that is

$$ax^2 + by^2 + cz^2 \equiv -4abc \pmod{32(abc)^2},$$

contradicting Theorem 1. Hence no such integers X, Y, Z exist. □

The following result follows immediately from Theorem 2.

Corollary 2. *Let $a, b, c \in \mathbb{N}$. Define positive integers r and s uniquely by*

$$abc = r^2 s, \quad s \text{ squarefree.}$$

Then the diagonal ternary quadratic form $ax^2 + by^2 + cz^2$ does not represent any of the positive integers

$$s(8abck - 1), \quad k \in \mathbb{N}.$$

Finally, we use Corollary 1 to give an arithmetic progression of positive integers not represented by the positive-definite ternary quadratic form $ax^2 + by^2 + cz^2 + dxy + exz + fyz$ thereby establishing the non-universality of the form.

Theorem 3. *Let $a, b, c, d, e, f \in \mathbb{Z}$ be such that the tenary quadratic form*

$$Q(x, y, z) := ax^2 + by^2 + cz^2 + dxy + exz + fyz$$

is positive-definite. Define integers Ω and Δ by

$$\Omega := 4ab - d^2, \quad \Delta := 4abc + def - (af^2 + be^2 + cd^2).$$

(Δ is the discriminant of $Q(x, y, z)$.) Further, define $R \in \mathbb{N}$ and $S \in \mathbb{Z}$ uniquely by

$$\Delta = R^2 S, \quad S \text{ squarefree.}$$

Then $Q(x, y, z)$ does not represent any of the integers

$$S(8a\Omega\Delta k - 1), \quad k \in \mathbb{N}.$$

Proof. As $Q(x, y, z)$ is positive-definite, we have that

$$a > 0, \quad \begin{vmatrix} a & \frac{d}{2} \\ \frac{d}{2} & b \end{vmatrix} > 0, \quad \begin{vmatrix} a & \frac{d}{2} & \frac{e}{2} \\ \frac{d}{2} & b & \frac{f}{2} \\ \frac{e}{2} & \frac{f}{2} & c \end{vmatrix} > 0,$$

so that Ω, Δ and S are positive integers. Using MAPLE (or similar software) it is easy to verify the following identity:

$$4a\Omega \cdot Q(x, y, z) = (\Omega y + (2af - de)z)^2 + \Omega(2ax + dy + ez)^2 + 4a\Delta z^2. \tag{1}$$

Let $k \in \mathbb{N}$. Suppose that X, Y and Z are integers such that

$$Q(X, Y, Z) = S(8a\Omega\Delta k - 1). \tag{2}$$

Define integers x, y and z by

$$x = R(\Omega Y + (2af - de)Z), \quad y = R(2aX + dY + eZ), \quad z = 2RZ. \tag{3}$$

Then

$$\begin{aligned} & x^2 + \Omega y^2 + a\Delta z^2 \\ & \quad = R^2 \left((\Omega Y + (2af - de)Z)^2 + \Omega (2aX + dY + eZ)^2 + 4a\Delta Z^2 \right) \\ & \quad = 4a\Omega R^2 Q(X, Y, Z) \end{aligned}$$

by (1), so that by (2) we have

$$x^2 + \Omega y^2 + a\Delta z^2 = 4a\Omega\Delta(8a\Omega\Delta k - 1).$$

This contradicts Corollary 1. Hence, for any $k \in \mathbb{N}$, $Q(x, y, z)$ does not represent $S(8a\Omega\Delta k - 1)$, and so $Q(x, y, z)$ is not universal. □

2. Number of Solutions

The remainder of this paper is dedicated to proving Theorem 1. In this section, we state the two propositions that will allow us to deduce the assertion of this theorem. For $a, b, c, k \in \mathbb{N}$ and $d \in \mathbb{Z}$, we let $N(a, b, c; d; k)$ denote the number of solutions of the congruence $ax^2 + by^2 + cz^2 \equiv d \pmod{k}$, that is

$$N(a, b, c; d; k) = \#\{(x, y, z) \in \mathbb{Z}_k^3 \mid ax^2 + by^2 + cz^2 \equiv d \pmod{k}\},$$

where $\mathbb{Z}_k$ denotes a complete set of residues modulo k. With this notation, our aim is to show that

$$N(a, b, c; -4abc; 32(abc)^2) = 0. \tag{4}$$

This problem can be simplified by the following classical result.

Proposition 1. *Let $a, b, c, k \in \mathbb{N}$. Let $k = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ be the prime decomposition of k. Then for any $d \in \mathbb{Z}$ we have*

$$N(a, b, c; d; k) = \prod_{i=1}^{n} N(a, b, c; d; p_i^{\alpha_i}).$$

One can prove Proposition 1 in a straightforward way using the Chinese remainder theorem (see [11], [9, pp. 171-177]). It follows from Proposition 1 that to prove (4) we must show there exists at least one prime p such that $p^m \mid\mid 32(abc)^2$ and $N(a, b, c; -4abc; p^m) = 0$. This will follow from the following two propositions, which are proved in Section 4.

It is convenient to introduce the following notation. For odd positive integers A, B and C we define

$$\lambda(A, B, C) = \begin{cases} 0 & \text{if } A \equiv B \equiv C \pmod{4}, \\ 1 & \text{otherwise.} \end{cases}$$

We also make use of the Jacobi symbol $\left(\frac{t}{k}\right)$ which is defined for a positive odd integer k and an integer t. Jacobi's law of quadratic reciprocity asserts that

$$\left(\frac{k}{l}\right)\left(\frac{l}{k}\right) = (-1)^{\frac{(k-1)}{2}\frac{(l-1)}{2}}$$

for positive odd coprime integers k and l. The two supplements to this law are $\left(\frac{-1}{k}\right) = (-1)^{\frac{k-1}{2}}$ and $\left(\frac{2}{k}\right) = (-1)^{\frac{k^2-1}{8}}$, valid for any positive odd integer k.

Proposition 2. *Let $a, b, c \in \mathbb{N}$. We write*

$$a = 2^\alpha A, \quad b = 2^\beta B, \quad c = 2^\gamma C,$$

where $A, B, C \in \mathbb{N}$ are odd and $\alpha, \beta, \gamma \in \mathbb{N}_0$. If

$$\left(\frac{2}{A}\right)^{\beta+\gamma}\left(\frac{2}{B}\right)^{\alpha+\gamma}\left(\frac{2}{C}\right)^{\alpha+\beta} = (-1)^{\lambda(A,B,C)} \tag{5}$$

then

$$N(a, b, c; -4abc; 2^{5+2(\alpha+\beta+\gamma)}) = 0.$$

Proposition 3. *Let $a, b, c \in \mathbb{N}$. We write*

$$a = 2^\alpha A, \quad b = 2^\beta B, \quad c = 2^\gamma C,$$

where $A, B, C \in \mathbb{N}$ are odd and $\alpha, \beta, \gamma \in \mathbb{N}_0$. If

$$\left(\frac{2}{A}\right)^{\beta+\gamma}\left(\frac{2}{B}\right)^{\alpha+\gamma}\left(\frac{2}{C}\right)^{\alpha+\beta} = (-1)^{\lambda(A,B,C)+1},$$

then there exists an odd prime p dividing at least one of a, b, c such that

$$N(a, b, c; -4abc; p^{2(\alpha_1+\beta_1+\gamma_1)}) = 0,$$

where $p^{\alpha_1} \mid\mid a$, $p^{\beta_1} \mid\mid b$, $p^{\gamma_1} \mid\mid c$.

The proof of Theorem 1 is immediate from Propositions 2 and 3.

3. Lemmas

In this section we prove three lemmas. The first lemma gives a basic congruence relation which is used in the proof of Proposition 2. The second lemma asserts that a certain Jacobi symbol has the value -1 and the third lemma establishes that a certain congruence has no solutions. Lemmas 2 and 3 are used in the proof of Proposition 3.

For $k \in \mathbb{N}$ we let $\{r_1, r_2, \ldots, r_n\}_k$ denote the set of residues $r_1, \ldots, r_n$ modulo k.

Lemma 1. *Let A, B, C be odd positive integers. Let $r, s, t \in \mathbb{N}_0$ be either all of the same parity or at most one of them is even. If*

$$\left(\frac{2}{A}\right)^{r+s}\left(\frac{2}{B}\right)^{r+t}\left(\frac{2}{C}\right)^{s+t} = (-1)^{\lambda(A,B,C)} \tag{6}$$

then $A + 2^r B + 2^s C \not\equiv -2^t ABC \pmod 8$.

Proof. Let $E := A + 2^r B + 2^s C + 2^t ABC$. We wish to show that $E \not\equiv 0 \pmod 8$ under condition (6).

Suppose first that $\lambda(A, B, C) = 0$. In this case $A \equiv B \equiv C \pmod 4$ and by the pigeon-hole principle we must have at least two of A, B, C congruent modulo 8. Then

$$\begin{aligned}
AE &\equiv AB(2^r + 2^s) + (1 + 2^t) \pmod 8 \quad \text{if} \quad B \equiv C \pmod 8,\\
BE &\equiv BC(1 + 2^s) + (2^r + 2^t) \pmod 8 \quad \text{if} \quad A \equiv C \pmod 8,\\
CE &\equiv AC(1 + 2^r) + (2^s + 2^t) \pmod 8 \quad \text{if} \quad A \equiv B \pmod 8.
\end{aligned} \tag{7}$$

We note that $AB \equiv AC \equiv BC \equiv 1 \pmod 4$ so that each of AB, BC, AC is congruent to 1 or 5 modulo 8. For $u, v \in \mathbb{N}_0$ we have

$$\begin{aligned}
1 + 2^u &\in \{1, 2, 5\}_8 && \text{if } u \text{ is even},\\
1 + 2^u &\in \{1, 3\}_8 && \text{if } u \text{ is odd},\\
2^u + 2^v &\in \{0, 1, 2, 4, 5\}_8 && \text{if } u, v \text{ are even},\\
2^u + 2^v &\in \{0, 2, 4\}_8 && \text{if } u, v \text{ are odd},\\
2^u + 2^v &\in \{0, 1, 2, 3, 4, 6\}_8 && \text{if } u, v \text{ are of opposite parity.}
\end{aligned}$$

Hence, if r, s, t are all of the same parity, from (7) we have $AE, BE, CE \not\equiv 0 \pmod 8$ according as $B \equiv C \pmod 8$, $A \equiv C \pmod 8$, $A \equiv B \pmod 8$ respectively, so that $E \not\equiv 0 \pmod 8$. If r is even and s, t odd then (6) gives $A \equiv B \pmod 8$ and from the third congruence in (7) we deduce that $CE \not\equiv 0 \pmod 8$ so $E \not\equiv 0 \pmod 8$. The remaining cases s even, r, t odd and t even, r, s odd follow in a similar manner from the second and first congruences in (7) respectively.

Now suppose that $\lambda(A, B, C) = 1$. Then from (6) we see that r, s, t cannot all be of the same parity. Thus exactly one of r, s and t is even. We treat the case s even and r, t odd as the other two cases can be handled similarly. For s even and r, t odd (6) yields $\left(\frac{2}{AC}\right) = -1$ so that

$$AC \equiv 3 \pmod 8 \quad \text{and} \quad A \not\equiv C \pmod 4 \tag{8}$$

or

$$AC \equiv 5 \pmod 8 \quad \text{and} \quad A \equiv C \pmod 4,\ A \not\equiv B \pmod 4. \tag{9}$$

Then

$$CE \equiv \begin{cases} AB(3 \cdot 2^r + 2^t) + (3 + 2^s) \pmod 8 & \text{in case (8)}, \\ AB(5 \cdot 2^r + 2^t) + (5 + 2^s) \pmod 8 & \text{in case (9)}. \end{cases}$$

Now as s is even we have

$$3 + 2^s \in \{3, 4, 7\}_8, \quad 5 + 2^s \in \{1, 5, 6\}_8,$$

and as r, t are odd we have

$$\begin{aligned} &AB(3 \cdot 2^r + 2^t) \in \{0, 2, 6\}_8, \\ &AB(5 \cdot 2^r + 2^t) \in \{0, 4, 6\}_8 \quad \text{if } A \not\equiv B \pmod 4, \end{aligned}$$

so that in both (8) and (9) we have $CE \not\equiv 0 \pmod 8$ so that $E \not\equiv 0 \pmod 8$. □

Lemma 2. *Let $A, B, C \in \mathbb{N}$ be squarefree and such that $(A, B, C) = 1$. At least one of A, B, C is odd so permuting A, B and C as necessary we may suppose without loss of generality that A is odd and $B = 2^\beta B', C = 2^\gamma C'$, where B' and C' are odd positive squarefree integers and $\beta, \gamma \in \{0, 1\}$ with $\beta \le \gamma$. Let $P, Q, \ldots, U$ be the odd positive squarefree integers defined as follows:*

$$\begin{aligned} &P := \frac{A}{(A, B'C')}, \quad Q := \frac{B'}{(B', AC')}, \quad R := \frac{C'}{(C', AB')}, \\ &S := (A, B'), \quad T := (A, C'), \quad U := (B', C'). \end{aligned}$$

If

$$\left(\frac{2}{A}\right)^{\beta+\gamma} \left(\frac{2}{B'}\right)^{\gamma} \left(\frac{2}{C'}\right)^{\beta} = (-1)^{\lambda(A,B',C')+1}$$

then at least one of

$$\begin{aligned} &\left(\frac{-BC}{P}\right), \quad \left(\frac{-AC}{Q}\right), \quad \left(\frac{-AB}{R}\right), \\ &\left(\frac{-AB/S^2}{S}\right), \quad \left(\frac{-AC/T^2}{T}\right), \quad \left(\frac{-BC/U^2}{U}\right), \end{aligned}$$

is -1.

Proof. We observe that P is either 1 or the product of the odd primes dividing A which do not divide $B'C'$, and similarly for Q and R. As well, S is either 1 or is the product of the odd primes dividing both A and B' but not C', and similarly for T and U. Also, we observe that $P, Q, \ldots, U$ are pairwise coprime. Further, we have

$$A = PST, \quad B = 2^\beta QSU, \quad C = 2^\gamma RTU.$$

We now assume that

$$1 = \left(\frac{-BC}{P}\right) = \left(\frac{-AC}{Q}\right) = \left(\frac{-AB}{R}\right)$$
$$= \left(\frac{-AB/S^2}{S}\right) = \left(\frac{-AC/T^2}{T}\right) = \left(\frac{-BC/U^2}{U}\right)$$

and obtain a contradiction. Hence,

$$1 = \left(\frac{-2^{\beta+\gamma}QRSTU^2}{P}\right) = \left(\frac{-2^{\gamma}PRST^2U}{Q}\right) = \left(\frac{-2^{\beta}PQS^2TU}{R}\right)$$
$$= \left(\frac{-2^{\beta}PQTU}{S}\right) = \left(\frac{-2^{\gamma}PRSU}{T}\right) = \left(\frac{-2^{\beta+\gamma}QRST}{U}\right). \tag{10}$$

As $P, \ldots, U$ are all odd positive pairwise coprime integers, using basic properties of the Jacobi symbol, (10) gives

$$1 = \left(\frac{-2^{\beta+\gamma}QRST}{PU}\right) = \left(\frac{-2^{\gamma}PRSU}{QT}\right) = \left(\frac{-2^{\beta}PQTU}{RS}\right).$$

Taking their product, we deduce

$$1 = \left(\frac{-2^{\beta+\gamma}QRST}{PU}\right)\left(\frac{-2^{\gamma}PRSU}{QT}\right)\left(\frac{-2^{\beta}PQTU}{RS}\right).$$

Hence, we have

$$1 = \left(\frac{-2^{\beta+\gamma}}{PU}\right)\left(\frac{-2^{\gamma}}{QT}\right)\left(\frac{-2^{\beta}}{RS}\right)\left(\frac{QRST}{PU}\right)\left(\frac{PRSU}{QT}\right)\left(\frac{PQTU}{RS}\right)$$

and thus

$$1 = \left(\frac{-1}{PU}\right)\left(\frac{-1}{QT}\right)\left(\frac{-1}{RS}\right)\left(\frac{2}{PU}\right)^{\beta+\gamma}\left(\frac{2}{QT}\right)^{\gamma}\left(\frac{2}{RS}\right)^{\beta}$$
$$\times \left(\frac{QT}{PU}\right)\left(\frac{PU}{QT}\right)\left(\frac{RS}{PU}\right)\left(\frac{PU}{RS}\right)\left(\frac{RS}{QT}\right)\left(\frac{QT}{RS}\right). \tag{11}$$

Applying the law of quadratic reciprocity, together with its two supplements, we can express the right hand side of (11) as a power of (-1). Hence, (11) yields a congruence modulo 2, which, when simplified slightly, is given by

$$0 \equiv \frac{(QT+1)}{2}\frac{(PU-1)}{2} + \frac{(RS-1)}{2}\frac{(PU+1)}{2} + \frac{(RS+1)}{2}\frac{(QT-1)}{2}$$
$$+ \frac{(\beta+\gamma)((PU)^2-1)}{8} + \frac{\gamma((QT)^2-1)}{8} + \frac{\beta((RS)^2-1)}{8} \pmod 2. \tag{12}$$

We now examine the congruence (12) under the conditions stated in the lemma.

Suppose first that $\lambda(A, B', C') = 0$; that is,

$$A \equiv B' \equiv C' \pmod 4 \quad \text{and} \quad \left(\frac{2}{A}\right)^{\beta+\gamma}\left(\frac{2}{B'}\right)^{\gamma}\left(\frac{2}{C'}\right)^{\beta} = -1.$$

We only treat the case $(\beta, \gamma) = (0, 1)$ as the case $(\beta, \gamma) = (1, 1)$ follows similarly. We have $\left(\frac{2}{AB'}\right) = -1$ and $A = PST, B' = QSU$ and $C' = RTU$ so that

$$-1 = \left(\frac{2}{PST \cdot QSU}\right) = \left(\frac{2}{PU}\right)\left(\frac{2}{QT}\right).$$

Hence

$$\frac{(PU)^2 - 1}{8} + \frac{(QT)^2 - 1}{8} \equiv 1 \pmod 2 \tag{13}$$

and

$$PQTU \equiv 3, 5 \pmod 8. \tag{14}$$

As $A \equiv B' \pmod 4$ we have $PT \equiv QU \pmod 4$ so that $PQTU \equiv 1 \pmod 4$ and thus by (14)

$$PQTU \equiv 5 \pmod 8. \tag{15}$$

Further, as $B' \equiv C' \pmod 4$ we have $QS \equiv RT \pmod 4$ so that

$$RS \equiv QT \pmod 4. \tag{16}$$

Using (13) in (12) we obtain

$$1 \equiv \frac{(QT+1)}{2}\frac{(PU-1)}{2} + \frac{(RS-1)}{2}\frac{(PU+1)}{2} + \frac{(RS+1)}{2}\frac{(QT-1)}{2} \pmod 2.$$

Multiplying this congruence by 4, we deduce

$$7 \equiv PQTU + PRSU + QRST \pmod 8.$$

Appealing to (15), we have

$$1 \equiv RS\left(\frac{PU+QT}{2}\right) \pmod 4.$$

Then, appealing to (16), we have

$$1 \equiv QT\left(\frac{PU+QT}{2}\right) \pmod 4.$$

Multiplying this congruence by 2, and making use of (15), we obtain the contradiction

$$2 \equiv PQTU + (QT)^2 \equiv 5 + 1 \equiv 6 \pmod 8.$$

Suppose now that $\lambda(A, B', C') = 1$, that is

$$A, B', C' \text{ not all congruent modulo 4} \quad \text{and} \quad \left(\frac{2}{A}\right)^{\beta+\gamma} \left(\frac{2}{B'}\right)^{\gamma} \left(\frac{2}{C'}\right)^{\beta} = 1.$$

We just treat the case $B' \equiv 1 \pmod 4$ and $C' \equiv 3 \pmod 4$ as the other cases can be handled in a similar manner. First suppose that $(\beta, \gamma) = (0, 0)$. Then (12) is given by

$$\frac{(QT+1)}{2}\frac{(PU-1)}{2} + \frac{(RS-1)}{2}\frac{(PU+1)}{2} + \frac{(RS+1)}{2}\frac{(QT-1)}{2} \equiv 0 \pmod 2. \tag{17}$$

Now

$$QSU = B' \equiv 1 \pmod 4 \quad \text{and} \quad RTU = C' \equiv 3 \pmod 4$$

so that

$$S \equiv QU \pmod 4 \quad \text{and} \quad T \equiv -RU \pmod 4.$$

Let $v = QRU$ and $w = PU$. Then

$$\begin{aligned}
\frac{(QT+1)}{2}\frac{(PU-1)}{2} &\equiv \frac{(1-v)}{2}\frac{(w-1)}{2} \equiv \frac{1}{4}(-1+v+w-vw) \pmod 2,\\
\frac{(RS-1)}{2}\frac{(PU+1)}{2} &\equiv \frac{(v-1)}{2}\frac{(w+1)}{2} \equiv \frac{1}{4}(-1+v-w+vw) \pmod 2,\\
\frac{(RS+1)}{2}\frac{(QT-1)}{2} &\equiv \frac{(v+1)}{2}\frac{(-v-1)}{2} \equiv \frac{1}{4}(-2v-2) \pmod 2,
\end{aligned}$$

so that

$$\begin{aligned}
\frac{(QT+1)}{2}\frac{(PU-1)}{2} + \frac{(RS-1)}{2}\frac{(PU+1)}{2} + \frac{(RS+1)}{2}\frac{(QT-1)}{2}&\\
\equiv \frac{1}{4}(-4) \equiv 1 \pmod 2,&
\end{aligned}$$

contradicting (17).

Thus we may suppose that $(\beta, \gamma) \neq (0, 0)$. We now treat the case $(\beta, \gamma) = (0, 1)$. The remaining case $(\beta, \gamma) = (1, 1)$ can be handled in a similar manner. In this case, we have $\left(\frac{2}{AB'}\right) = 1$. Hence $AB' \equiv \pm 1 \pmod 8$. If

$$A \equiv B' \pmod 4 \quad \text{then} \quad AB' \equiv 1 \pmod 8$$

and if

$$A \not\equiv B' \pmod 4 \quad \text{then} \quad AB' \equiv 7 \pmod 8.$$

We just treat the case $A \equiv B' \pmod 4$ as the other case follows in a similar manner. As $AB' \equiv 1 \pmod 8$ we have

$$PQTU \equiv 1 \pmod 8. \tag{18}$$

As $A \equiv B' \pmod 4$, we have $B' \not\equiv C' \pmod 4$ since A, B', C' are not all congruent modulo 4. Thus, $B' \equiv -C' \pmod 4$. Hence, as $B' = QSU$ and $C' = RTU$, we deduce that $QS \equiv -RT \pmod 4$, and so

$$QT \equiv -RS \pmod 4. \tag{19}$$

Next

$$\left(\frac{2}{PU}\right)\left(\frac{2}{QT}\right) = \left(\frac{2}{PST \cdot QSU}\right) = \left(\frac{2}{AB'}\right) = 1,$$

so that

$$\frac{(PU)^2-1}{8} + \frac{(QT)^2-1}{8} \equiv 0 \pmod 2.$$

Hence (12) becomes

$$0 \equiv \frac{(QT+1)}{2}\frac{(PU-1)}{2} + \frac{(RS-1)}{2}\frac{(PU+1)}{2} + \frac{(RS+1)}{2}\frac{(QT-1)}{2} \pmod 2.$$

Multiplying this congruence by 4, we deduce

$$3 \equiv PQTU + PRSU + QRST \pmod 8.$$

Appealing to (18) we have

$$1 \equiv RS\left(\frac{PU+QT}{2}\right) \pmod 4.$$

Then, appealing to (19), we have

$$1 \equiv -QT\left(\frac{PU+QT}{2}\right) \pmod 4.$$

Multiplying this congruence by 2, and making use of (18), we obtain the contradiction

$$2 \equiv -PQTU - (QT)^2 \equiv -1 - 1 \equiv 6 \pmod 8.$$

This proves the lemma. □

Lemma 3. *Let $a, b, c \in \mathbb{N}$ and p be an odd prime. Write*

$$a = p^{\alpha}A, \quad b = p^{\beta}B, \quad c = p^{\gamma}C,$$

for some $\alpha, \beta, \gamma \in \mathbb{N}_0$ and $A, B, C \in \mathbb{N}$ coprime to p. If α, β, γ are not all congruent modulo 2 and

$$\left(\frac{A}{p}\right)^{\beta+\gamma}\left(\frac{B}{p}\right)^{\alpha+\gamma}\left(\frac{C}{p}\right)^{\alpha+\beta} = -\left(\frac{-1}{p}\right), \tag{20}$$

then

$$N(a, b, c; -4abc; p^{2(\alpha+\beta+\gamma)}) = 0.$$

Proof. Suppose that $(x, y, z) \in \mathbb{Z}^3$ is such that

$$ax^2 + by^2 + cz^2 \equiv -4abc \pmod{p^{2(\alpha+\beta+\gamma)}}. \tag{21}$$

We may suppose that each of x, y and z lies in $\{1, 2, \ldots, p^{2(\alpha+\beta+\gamma)}\}$. We write $x = p^j X, y = p^k Y, z = p^l Z$, where $j, k, l \in \mathbb{N}_0$ satisfy $j, k, l \leq 2(\alpha+\beta+\gamma)$ and $X, Y, Z \in \mathbb{N}$ are coprime to p and satisfy $X \leq p^{2(\alpha+\beta+\gamma)-j}, Y \leq p^{2(\alpha+\beta+\gamma)-k}$, $Z \leq p^{2(\alpha+\beta+\gamma)-l}$. Let

$$E := p^{\alpha+2j}AX^2 + p^{\beta+2k}BY^2 + p^{\gamma+2l}CZ^2 + 4p^{\alpha+\beta+\gamma}ABC. \tag{22}$$

By (21) and (22) we have

$$E \equiv 0 \pmod{p^{2(\alpha+\beta+\gamma)}}. \tag{23}$$

If $\min(\alpha+2j, \beta+2k, \gamma+2k) > \alpha+\beta+\gamma$ then

$$p^{\alpha+\beta+\gamma} \mid\mid E. \tag{24}$$

As α, β, γ are not all congruent modulo 2, at least one of them is odd, and so at least one of them is positive. Hence $\alpha+\beta+\gamma > 0$ and so $2(\alpha+\beta+\gamma) > \alpha+\beta+\gamma$. Then from (24) we have $p^{2(\alpha+\beta+\gamma)} \nmid E$ which contradicts (23). Thus

$$\min(\alpha+2j, \beta+2k, \gamma+2l) \leq \alpha+\beta+\gamma.$$

We only treat the case

$$\min(\alpha+2j, \beta+2k, \gamma+2l) = \alpha+2j$$

as the other two cases can be handled similarly. In this case, we have

$$\alpha+2j \leq \beta+2k, \quad \alpha+2j \leq \gamma+2l, \quad \alpha+2j \leq \alpha+\beta+\gamma. \tag{25}$$

We now just treat the case $(\alpha,\beta,\gamma)\equiv(0,1,1) \pmod 2$ as the other cases follow in a similar manner. From (20) we obtain $\left(\frac{BC}{p}\right) = -\left(\frac{-1}{p}\right)$. From (22) and (25) we deduce that

$$E = p^{\alpha+2j}E_1 = p^{\alpha+2j}\left(AX^2 + p^rBY^2 + p^sCZ^2 + 4p^tABC\right), \tag{26}$$

where $r,s,t \in \mathbb{N}_0$ and $(r,s,t)\equiv(1,1,0) \pmod 2$. We now show that $p \nmid E_1$. Suppose $p \mid E_1$. As $r,s \geq 1$ from (26) we see that

$$AX^2 + 4p^tABC \equiv 0 \pmod p.$$

As $(A,p)=1$ it follows that

$$X^2 + 4p^tBC \equiv 0 \pmod p.$$

As $(X,p)=1$ we must have $(4p^tBC,p)=1$ so $t=0$. Then $X^2 \equiv -4BC \pmod p$ and so $\left(\frac{-4BC}{p}\right) = 1$, contradicting $\left(\frac{BC}{p}\right) = -\left(\frac{-1}{p}\right)$. Hence $p \nmid E_1$ and so $p^{\alpha+2j} \mid\mid E$. But

$$\alpha + 2j \leq \alpha+\beta+\gamma < 2(\alpha+\beta+\gamma),$$

so $p^{2(\alpha+\beta+\gamma)} \nmid E$, contradicting (23). Hence (21) is insolvable. □

4. Proof of Propositions

In this section we present the proofs of Propositions 2 and 3, the necessary propositions we used to prove Theorem 1 in Section 2.

Proof of Proposition 2. Suppose that $(x,y,z) \in \mathbb{Z}^3$ is such that

$$ax^2 + by^2 + cz^2 \equiv -4abc \pmod{2^{5+2(\alpha+\beta+\gamma)}}. \tag{27}$$

We may suppose that each of x,y and z lies in $\{1,2,\ldots,2^{5+2(\alpha+\beta+\gamma)}\}$. Then we write $x=2^jX$, $y=2^kY$, $z=2^lZ$, where $j,k,l \in \mathbb{N}_0$, $X,Y,Z \in \mathbb{N}$, X,Y,Z are odd, and $X \leq 2^{5+2(\alpha+\beta+\gamma)-j}$, $Y \leq 2^{5+2(\alpha+\beta+\gamma)-k}$, $Z \leq 2^{5+2(\alpha+\beta+\gamma)-l}$. Let

$$E := 2^{\alpha+2j}AX^2 + 2^{\beta+2k}BY^2 + 2^{\gamma+2l}CZ^2 + 2^{2+\alpha+\beta+\gamma}ABC. \tag{28}$$

By (27) and (28) we have

$$E \equiv 0 \pmod{2^{5+2(\alpha+\beta+\gamma)}}. \tag{29}$$

If

$$\min(\alpha+2j,\beta+2k,\gamma+2l) > 2+\alpha+\beta+\gamma$$

then

$$E \equiv 2^{2+\alpha+\beta+\gamma}ABC \pmod{2^{3+\alpha+\beta+\gamma}},$$

contradicting (29). Hence $\min(\alpha+2j,\beta+2k,\gamma+2l) \leq 2+\alpha+\beta+\gamma$. We treat the case $\min(\alpha+2j,\beta+2k,\gamma+2l) = \alpha+2j$ as the other two cases can be handled similarly. In this case, we have

$$\alpha+2j \leq \beta+2k, \quad \alpha+2j \leq \gamma+2l, \quad \alpha+2j \leq 2+\alpha+\beta+\gamma. \tag{30}$$

Suppose first that $\lambda(A,B,C)=0$. In this case, we have $A \equiv B \equiv C \pmod 4$. We just treat the case $\alpha \equiv \beta \equiv \gamma \pmod 2$ as the other cases arising from (5) follow in a similar manner. From (28) and (30) we have

$$E = 2^{\alpha+2j}E_1 = 2^{\alpha+2j}(AX^2+2^rBY^2+2^sCZ^2+2^tABC),$$

where

$$\begin{aligned} r &= \beta-\alpha+2k-2j \in \mathbb{N}_0, \quad r \equiv 0 \pmod 2,\\ s &= \gamma-\alpha+2l-2j \in \mathbb{N}_0, \quad s \equiv 0 \pmod 2,\\ t &= 2+\beta+\gamma-2j \in \mathbb{N}_0, \quad t \equiv 0 \pmod 2. \end{aligned}$$

Then from Lemma 1 we deduce that

$$E_1 \not\equiv 0 \pmod 8 \quad \text{ so that } \quad E \not\equiv 0 \pmod{2^{3+\alpha+2j}}.$$

Appealing to (30) we deduce

$$5+2(\alpha+\beta+\gamma) \geq 5+\alpha+\beta+\gamma \geq 3+\alpha+2j$$

so that $E \not\equiv 0 \pmod{2^{5+2(\alpha+\beta+\gamma)}}$, contradicting (29).

Now suppose $\lambda(A,B,C)=1$. We only treat the case $(\alpha,\beta,\gamma) \equiv (0,1,1) \pmod 2$, as the other cases follow in a similar manner. In this case, we have

$$A,B,C \text{ are not all congruent modulo } 4 \quad \text{ and } \quad \left(\frac{2}{BC}\right) = -1.$$

From (28) and (30) we have

$$E = 2^{\alpha+2j}E_1 = 2^{\alpha+2j}(AX^2+2^rBY^2+2^sCZ^2+2^tABC),$$

where $r,s,t \in \mathbb{N}_0$ and $(r,s,t) \equiv (1,1,0) \pmod 2$. By Lemma 1 we deduce that $E_1 \not\equiv 0 \pmod 8$ so that $E \not\equiv 0 \pmod{2^{3+\alpha+2j}}$, and as before we obtain the contradiction $E \not\equiv 0 \pmod{2^{5+2(\alpha+\beta+\gamma)}}$. Thus the congruence (27) is insolvable. □

Proof of Proposition 3. Without loss of generality we may suppose that $\alpha \le \beta \le \gamma$. Let $(a,b,c) = 2^\sigma \zeta$, where $\sigma \in \mathbb{N}_0$ and $\zeta \in \mathbb{N}$ is odd. Now, as $\alpha \le \beta \le \gamma$ and A is odd, we have

$$(a,b,c) = (2^\alpha A, 2^\beta B, 2^\gamma C) = 2^\alpha (A,B,C),$$

so that $\sigma = \alpha$ and $\zeta = (A,B,C)$. Next, let r^2, s^2, t^2 denote the largest squares dividing $\dfrac{A}{(A,B,C)}, \dfrac{B}{(A,B,C)}, \dfrac{C}{(A,B,C)}$ respectively. As A,B,C are all odd, so are r,s,t. Moreover, there exist odd squarefree positive integers $\tilde{A}, \tilde{B}, \tilde{C}$ such that

$$\frac{A}{\zeta} = \tilde{A} r^2, \quad \frac{B}{\zeta} = \tilde{B} s^2, \quad \frac{C}{\zeta} = \tilde{C} t^2.$$

As $\zeta = (A,B,C)$ we have $(\tilde{A}, \tilde{B}, \tilde{C}) = (r,s,t) = 1$. Define $\beta_3, \gamma_3 \in \{0,1\}$ and $\beta_2, \gamma_2 \in \mathbb{N}_0$ by

$$\beta - \alpha = 2\beta_2 + \beta_3, \quad \gamma - \alpha = 2\gamma_2 + \gamma_3.$$

Hence,

$$\begin{aligned} a &= 2^\alpha A = 2^\alpha \zeta \tilde{A} r^2 = 2^\alpha \zeta \cdot \tilde{A} r^2, \\ b &= 2^\beta B = 2^{\alpha+2\beta_2+\beta_3} \zeta \tilde{B} s^2 = 2^\alpha \zeta \cdot 2^{\beta_3+2\beta_2} \tilde{B} s^2, \\ c &= 2^\gamma C = 2^{\alpha+2\gamma_2+\gamma_3} \zeta \tilde{C} t^2 = 2^\alpha \zeta \cdot 2^{\gamma_3+2\gamma_2} \tilde{C} t^2. \end{aligned}$$

We observe that (as r,s,t,ζ are odd),

$$\begin{aligned} A \equiv B \equiv C \pmod 4 &\iff \zeta \tilde{A} r^2 \equiv \zeta \tilde{B} s^2 \equiv \zeta \tilde{C} t^2 \pmod 4 \\ &\iff \zeta \tilde{A} \equiv \zeta \tilde{B} \equiv \zeta \tilde{C} \pmod 4 \\ &\iff \tilde{A} \equiv \tilde{B} \equiv \tilde{C} \pmod 4, \end{aligned}$$

so that $\lambda(A,B,C) = \lambda(\tilde{A}, \tilde{B}, \tilde{C})$. Also

$$\begin{aligned} &\left(\frac{2}{A}\right)^{\beta+\gamma} \left(\frac{2}{B}\right)^{\alpha+\gamma} \left(\frac{2}{C}\right)^{\alpha+\beta} \\ &= \left(\frac{2}{A}\right)^{(\alpha+2\beta_2+\beta_3)+(\alpha+2\gamma_2+\gamma_3)} \left(\frac{2}{B}\right)^{\alpha+(\alpha+2\gamma_2+\gamma_3)} \left(\frac{2}{C}\right)^{\alpha+(\alpha+2\beta_2+\beta_3)} \\ &= \left(\frac{2}{A}\right)^{\beta_3+\gamma_3} \left(\frac{2}{B}\right)^{\gamma_3} \left(\frac{2}{C}\right)^{\beta_3} = \left(\frac{2}{\zeta \tilde{A} r^2}\right)^{\beta_3+\gamma_3} \left(\frac{2}{\zeta \tilde{B} s^2}\right)^{\gamma_3} \left(\frac{2}{\zeta \tilde{C} t^2}\right)^{\beta_3} \\ &= \left(\frac{2}{\zeta}\right)^{\beta_3+\gamma_3+\gamma_3+\beta_3} \left(\frac{2}{\tilde{A}}\right)^{\beta_3+\gamma_3} \left(\frac{2}{\tilde{B}}\right)^{\gamma_3} \left(\frac{2}{\tilde{C}}\right)^{\beta_3}, \end{aligned}$$

so that

$$\left(\frac{2}{A}\right)^{\beta+\gamma} \left(\frac{2}{B}\right)^{\alpha+\gamma} \left(\frac{2}{C}\right)^{\alpha+\beta} = \left(\frac{2}{\tilde{A}}\right)^{\beta_3+\gamma_3} \left(\frac{2}{\tilde{B}}\right)^{\gamma_3} \left(\frac{2}{\tilde{C}}\right)^{\beta_3}.$$

We now assume that

$$\left(\frac{2}{A}\right)^{\beta+\gamma}\left(\frac{2}{B}\right)^{\alpha+\gamma}\left(\frac{2}{C}\right)^{\alpha+\beta}=(-1)^{\lambda(A,B,C)+1},$$

which means we have

$$\left(\frac{2}{\tilde{A}}\right)^{\beta_3+\gamma_3}\left(\frac{2}{\tilde{B}}\right)^{\gamma_3}\left(\frac{2}{\tilde{C}}\right)^{\beta_3}=(-1)^{\lambda(\tilde{A},\tilde{B},\tilde{C})+1}. \tag{31}$$

Thus, we cannot have $(\tilde{A},\tilde{B},\tilde{C})=(1,1,1)$. Hence, $(\tilde{A},\tilde{B},\tilde{C})\neq(1,1,1)$ and so as $\tilde{A},\tilde{B}$ and $\tilde{C}$ are all odd there is at least one odd prime p dividing at least one of $\tilde{A},\tilde{B}$ and $\tilde{C}$. As $(\tilde{A},\tilde{B},\tilde{C})=1$ we see that p divides either one or two of $\tilde{A},\tilde{B}$ and $\tilde{C}$. Let $v_p(m)$ denote the exponent of the exact power of p dividing the positive integer m. As $\tilde{A},\tilde{B}$ and $\tilde{C}$ are squarefree, we have

$$v_p(\tilde{A}),v_p(\tilde{B}),v_p(\tilde{C})=0,0,1 \text{ or } 0,1,1 \text{ in some order.}$$

Let $v_p(a)=\alpha_1,v_p(b)=\beta_1,v_p(c)=\gamma_1$, where $\alpha_1,\beta_1,\gamma_1\in\mathbb{N}_0$, so that $a=p^{\alpha_1}A_1$, $b=p^{\beta_1}B_1,c=p^{\gamma_1}C_1$ for some positive integers A_1,B_1,C_1 each coprime to p. As p divides at least one of $\tilde{A},\tilde{B}$ and $\tilde{C}$, p divides at least one of a,b and c, so at least one of α_1,β_1 and γ_1 is nonzero. We have

$$2^{\alpha}\zeta\cdot\tilde{A}r^2=p^{\alpha_1}A_1,\quad 2^{\alpha}\zeta\cdot 2^{\beta_3+2\beta_2}\tilde{B}s^2=p^{\beta_1}B_1,\quad 2^{\alpha}\zeta\cdot 2^{\gamma_3+2\gamma_2}\tilde{C}t^2=p^{\gamma_1}C_1.$$

Hence, setting $z=v_p(\zeta)$ we have that

$$\alpha_1\equiv z+v_p(\tilde{A}),\quad \beta_1\equiv z+v_p(\tilde{B}),\quad \gamma_1\equiv z+v_p(\tilde{C})\pmod 2,$$

and so α_1,β_1 and γ_1 are not all of the same parity. Applying Lemma 2 to $\tilde{A}$, $2^{\beta_3}\tilde{B}$, $2^{\gamma_3}\tilde{C}$, we deduce in view of (31) that at least one of

$$\left(\frac{-2^{\beta_3+\gamma_3}\tilde{B}\tilde{C}}{P}\right),\quad \left(\frac{-2^{\gamma_3}\tilde{A}\tilde{C}}{Q}\right),\quad \left(\frac{-2^{\beta_3}\tilde{A}\tilde{B}}{R}\right),$$
$$\left(\frac{-2^{\beta_3}\tilde{A}\tilde{B}/S^2}{S}\right),\quad \left(\frac{-2^{\gamma_3}\tilde{A}\tilde{C}/T^2}{T}\right),\quad \left(\frac{-2^{\beta_3+\gamma_3}\tilde{B}\tilde{C}/U^2}{U}\right),$$

is -1, where (with empty products $=1$)

$$P=\prod_{\substack{p\mid\tilde{A}\\ p\nmid\tilde{B}\tilde{C}}}p,\quad Q=\prod_{\substack{p\mid\tilde{B}\\ p\nmid\tilde{A}\tilde{C}}}p,\quad R=\prod_{\substack{p\mid\tilde{C}\\ p\nmid\tilde{A}\tilde{B}}}p,$$
$$S=\prod_{\substack{p\mid\tilde{A},p\mid\tilde{B}\\ p\nmid\tilde{C}}}p,\quad T=\prod_{\substack{p\mid\tilde{A},p\mid\tilde{C}\\ p\nmid\tilde{B}}}p,\quad U=\prod_{\substack{p\mid\tilde{B},p\mid\tilde{C}\\ p\nmid\tilde{A}}}p.$$

If $\left(\dfrac{-2^{\beta_3+\gamma_3}\tilde{B}\tilde{C}}{P}\right) = -1$ then there exists an odd prime p such that $p \mid \tilde{A}$, $p \nmid \tilde{B}\tilde{C}$ and $\left(\dfrac{-2^{\beta_3+\gamma_3}\tilde{B}\tilde{C}}{p}\right) = -1$. In this case, we have $v_p(\tilde{A}) = 1$ and $v_p(\tilde{B}) = v_p(\tilde{C}) = 0$ so that $\alpha_1 \not\equiv \beta_1 \equiv \gamma_1 \pmod 2$. Hence, as $\left(\dfrac{-2^{\beta_3+\gamma_3}\tilde{B}\tilde{C}}{p}\right) = -1$ it follows that

$$\left(\frac{A_1}{p}\right)^{\beta_1+\gamma_1}\left(\frac{B_1}{p}\right)^{\alpha_1+\gamma_1}\left(\frac{C_1}{p}\right)^{\alpha_1+\beta_1} = \left(\frac{B_1C_1}{p}\right) = \left(\frac{2^{\beta_3+\gamma_3}\tilde{B}\tilde{C}}{p}\right) = -\left(\frac{-1}{p}\right),$$

and so by Lemma 3, $N(a,b,c;-4abc;p^{2(\alpha_1+\beta_1+\gamma_1)}) = 0$. By similar reasoning, we reach the same conclusion if instead we have either $\left(\dfrac{-2^{\gamma_3}\tilde{A}\tilde{C}}{Q}\right) = -1$ or $\left(\dfrac{-2^{\beta_3}\tilde{A}\tilde{B}}{R}\right) = -1$. Suppose now that $\left(\dfrac{-2^{\beta_3}\tilde{A}\tilde{B}/S^2}{S}\right) = -1$. Then there exists an odd prime p such that $p \mid \tilde{A}$, $p \mid \tilde{B}$ and $p \nmid \tilde{C}$. Similar to before we deduce that $\gamma_1 \not\equiv \alpha_1 \equiv \beta_1 \pmod 2$. Thus,

$$\left(\frac{A_1}{p}\right)^{\beta_1+\gamma_1}\left(\frac{B_1}{p}\right)^{\alpha_1+\gamma_1}\left(\frac{C_1}{p}\right)^{\alpha_1+\beta_1} = \left(\frac{A_1B_1}{p}\right) = \left(\frac{2^{\beta_3}\tilde{A}\tilde{B}/S^2}{p}\right) = -\left(\frac{-1}{p}\right),$$

and by Lemma 3 we have $N(a,b,c;-4abc;p^{2(\alpha_1+\beta_1+\gamma_1)}) = 0$. By similar reasoning, we reach the same conclusion if instead we have either $\left(\dfrac{-2^{\gamma_3}\tilde{A}\tilde{C}/T^2}{T}\right) = -1$ or $\left(\dfrac{-2^{\beta_3+\gamma_3}\tilde{B}\tilde{C}/U^2}{U}\right) = -1$. This proves the proposition. □

5. Final Remarks

Although the study of ternary quadratic forms is a classical one, it remains one of vital interest today. For example, Rouse's 451-theorem [10, Theorem 2, p. 1696] assumes the truth of the conjecture that each of the three ternary quadratic forms

$$x^2+2y^2+5z^2+xz,\ \ x^2+3y^2+6z^2+xy+2yz \quad \text{and} \quad x^2+3y^2+7z^2+xy+xz$$

represents all positive odd integers. Rouse [10, p. 1695] points out that there is at present no general algorithm for determining the integers represented by a positive-definite ternary quadratic form. Determining an explicit formula for the number of representations of a positive integer n by a ternary form Q is an active area of

research, see for example, Guo, Peng and Qin [6] for results in this direction. Even the determination of the positive integers represented by a particular form such as $x^2+7y^2+49z^2$ has important consequences in other branches of mathematics, see for example, Qin [8].

Finally, we indicate briefly how we determined the arithmetic conditions in Lemma 3 and Propositions 2 and 3. We started with

$$N(a,b,c;-4abc;p^n) = \frac{1}{p^n}\sum_{x,y,z=0}^{p^n-1}\sum_{w=0}^{p^n-1}\exp\left(2\pi i\cdot\frac{w(ax^2+by^2+cz^2+4abc)}{p^n}\right)$$
$$= \frac{1}{p^n}\sum_{w=0}^{p^n-1}\exp\left(2\pi i\cdot\frac{4abcw}{p^n}\right)\prod_{j=a,b,c}\sum_{x=0}^{p^n-1}\exp\left(2\pi i\cdot\frac{wjx^2}{p^n}\right),$$

where p is a prime and $n\in\mathbb{N}$. Each exponential sum $\displaystyle\sum_{x=0}^{p^n-1}\exp\left(2\pi i\frac{wjx^2}{p^n}\right)$ is a quadratic Gauss sum, whose evaluation is well known [2, p. 15]. Using these evaluations, after a long calculation, we were led to the arithmetic conditions in Lemma 3 and Propositions 2 and 3.

References

[1] A. A. Albert, The integers represented by sets of ternary quadratic forms, *Amer. J. Math.* **55** (1933), 274-292. [Collected Mathematical Papers of A. Adrian Albert. Part II, American Mathematical Society, Providence, RI, 1993. 57-75.]

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, Inc., New York, 1998.

[3] J. H. Conway, *The Sensual (Quadratic) Form*, The Carus Mathematical Monographs. No. 26, Mathematical Association of America, Washington, DC, 2005.

[4] L. E. Dickson, *Modern Elementary Theory of Numbers*, University of Chicago Press, Chicago, 1939.

[5] L. E. Dickson, *History of the Theory of Numbers, Vols. I-III*, Chelsea, New York, 1966.

[6] X. Guo, Y. Peng and H. Qin, On the representation numbers of ternary quadratic forms and modular forms of weight 3/2, *J. Number Theory* **140** (2014), 235-266.

[7] I. Kaplansky, Ternary positive quadratic forms that represent all odd positive-integers, *Acta. Arith.* **70** (1995), 209-214.

[8] H. Qin, Representation of integers by positive ternary quadratic forms, *Preprint*, 2016.

[9] K. H. Rosen, *Elementary Number Theory & its Applications*, Addison Wesley, sixth ed. 2011.

[10] J. Rouse, Quadratic forms representing all odd positive integers, *Amer. J. Math.* **136** (2014), 1693-1745.

[11] S. A. Stepanov, *Congruence with several variables*, in Encyclopedia of Mathematics, Springer, 2011. https://www.encyclopediaofmath.org/index.php/Congruence_with_several_variables